COMMONWEALTH OFFICE OF TECHNOLOGY

COT Security Alert – Web Site Defacement

This alert is being provided to bring additional awareness to security threats facing the Commonwealth of Kentucky.

Over the past couple of weeks, the COT Security Administration Branch has observed an increasing amount of attacks targeting web servers hosted on the **ky.gov** domain. These attacks, known as a web-site defacement, attempt to exploit holes in a websites security in order to overwrite the web page and display a banner touting the success of the attacker. Although these threats have not been observed to be targeting any specific individuals, machines, or agencies, increased vigilance is needed to protect critical IT resources in the face of an observed, growing trend in these attacks. While most of these attacks have had little to no success, the impact of such an attack (if successful) could have far-reaching implications.

COT is requesting that all web site administrators be vigilant and ensure that their web servers are protected. Some common methods used to secure web servers include:

1. Ensuring the system has the latest operating system and application patches installed.
2. Remove/disable any services/applications/scripting technologies that are not required.
3. Disable remote administration of the Web site (use a VPN to connect in and make changes).
4. Enforce the use of strong passwords on the web server and change them regularly.
5. Remove any default configurations that may come with an application/server (e.g. admin accounts).
6. Implement an application level firewall to restrict access to only those services required to be available for public use
7. Monitor all sites for unauthorized changes. Regularly review logs for suspicious activity.
8. Ensure industry standard secure coding practices are used in the development of new web pages. See www.owasp.org for additional details / suggestions.

9. Disable any directories / virtual directories that are not currently being used.
10. Request a web application security test be conducted on your site to identify any security shortcomings and resolve them proactively.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/ciso/